REMARKS/ARGUMENTS

Applicants have amended the claims to more particularly point out the claimed subject matter and thereby remove the various claim objections and rejections set forth on pages 1-6 of the Office Action. In particular, applicants have amended their claims to remove the objections alleging indefiniteness, improper antecedent basis and non-statutory subject matter. For example, applicants have amended claim 67, 68, etc. to provide proper antecedent basis, and have amended claims 104-121 & 125 to more surely recite statutory subject matter. Applicants do not understand the 112 rejection with respect to claims 78-86 and 90-103 (page 6 of Office Action) and request clarification. Applicants have also further amended claims 67, 69 and 107 to overcome the 112, fourth paragraph rejection.

Applicants believe their amendments herein should take care of all of the various objections and rejections to the form and format of the claims that the Examiner has set forth. However, should the Examiner believe that further claim amendments are necessary or desirable, he is requested to contact the undersigned by telephone to discuss same and reach agreement.

Applicants have also added new claims 126-134 to claim different scopes of protection to more adequately protect the claimed subject matter. Applicants request the Examiner to reconsider this application in view of the amendments and the following remarks.

Turning to the obviousness rejection, the exemplary illustrative non-limiting implementation disclosed in the present application provides an advantage of having a file index to allow the ordered and convenient storage of and access to multiple items of

information on the storage device without compromising the security of the encoding system.

Each of the independent claims 64, 65, 104, 115, 124 currently on file relate to claimed subject matter where data is stored in a file of random data on a storage device in the following way. First, a location for storing a file index is determined based on a user input passphrase. The file index is encrypted and stored at this location. Then, a location for storing a data set is decided and data is encrypted and stored at this location and an indication of the location where the data set is stored is noted in the file index by making an appropriate entry.

This whole process means that when a storage device carrying such a file of random data is inspected it cannot be easily determined whether or not any data is present on the storage device. Throughout the file there will be "random data" – either from the original file of random data or that which is stored encrypted data. There is just no indication of the presence of data or otherwise.

Moreover, where as in the present claims 64, 65, 104, 115, 124 the location of the passphrase is not fixed, if an attempt is made to try and crack the encoding then there is no logical starting place. This is because the location of the file index is variable. Thus, a person trying to crack the encoding to see whether any data is present or to obtain access to the data does not know where to begin in trying to determine whether there is an encrypted file index or encrypted data on the device.

This improves security over a case where the storage mechanism necessitates including some type of header or index which is always located at the start of the file.

None of the prior art cited by the Examiner discloses, teaches nor suggests any such type of solution as claimed herein in independent claims 64, 65, 104, 115, 124.

As recognized in the introduction of US 6011849 (Orrin), steganography, when it comes to its use in computers, generally consists of hiding information in graphical images, sound files or other media files where small changes in those files are relatively difficult to detect. The changes generally take the form of changing the least significant bits of bytes in the media file. While there may be some difficulty in detecting those changes if the media file is given a cursory review, if a concerted effort is made, it is actually quite straight forward to detect those changes.

Orrin proposes a modified system of hiding data in large media files in a similar way. It should also be noted that Orrin is related to the transfer of information and data in a secure way. This is made clear in the "Field of Invention" in column 1 of Orrin, as well as throughout the document. Thus, the methodology in Orrin is to hide a relatively small amount of data in a large media file or a large file of random data and then to transmit that by one route or another between entities. Thus, Orrin does not consider nor contemplate at all the idea of storing multiple items of data in a randomly accessible way as is facilitated by the subject matter claimed herein in independent claims 64, 65, 104, 115, 124. Moreover, the techniques in Orrin are inherently unsuitable for such usage.

In Orrin, as is shown in Figures 3, 4 and 5 and explained in the accompanying description, the following process takes place. The data which is to be transported is encrypted. This encrypted data is then "steg encoded". This involves taking a media file, which might be a file of random data, as a location in which to hide the data. This

"hiding" process is conducted by selecting bytes from the media file/file of random data using a selection cipher text which has been generated from a key. Then, the least significant bit of each selected byte (i.e. selected using the key) is bit converted to represent a bit of the encrypted data. Thus, in effect, one piece of data is broken down into bits (in the binary sense) and these bits are spread across a large file at locations determined by the key.

In the system of Orrin, if it was decided to encode more data it is submitted that this would be done in exactly the same way. That is to say, a larger initial payload of data would be collated and this would be similarly encrypted and steg encoded using the same technique. The location at which each bit of the encrypted data would be stored would be determined by the overall key. Thus, in such a situation there would be no file index and moreover no file index which is stored at a location determined by a passphrase or key. Rather there would be one continuous block of data which would be encoded for transmission using the system of Orrin and decoded after reception.

Using a file index in Orrin makes no sense. The location of data in Orrin is determined by a key. If data to be stored in Orrin included a file index this would also be broken down by the same encoding process and stored bit wise in multiple locations. This would serve no useful purpose until all the data was decoded and decrypted. This is because up until that point, all the data storage locations would be determined by the overall key. There would be no individually accessible file index which could be decrypted and decoded, and similarly no individually accessible items of data which could be accessed.

If one were to decide to try and combine use of a file index with Orrin, then to arrive at the subject matter claimed herein in independent claims 64, 65, 104, 115, 124 the following steps would have to be taken. First of all, of course, a decision would have to be made to use a file index which, as already suggested, seems to be counter intuitive. Then a decision must be made to encrypt that index. Then one must consider what entries would be made in the index. Perhaps this would specify a starting point within the file for encoding each data set. However, with the encoding method of Orrin where each piece of data is split down to bits and encoded at separate locations determined by a key, it must be questioned whether this is a sensible and necessary step at all.

Further, to arrive at the existing independent claims 64, 65, 104, 115, 124, even if all of these steps are taken then there must also be a decision to use a method where the location of the file index is based on a passphrase. It is submitted that there is no teaching whatsoever in the prior art to take this insightful step of locating the file index at a variable location.

If a file index were to be provided in Orrin, the natural thing to do would be to provide the file index at the start of the file.

It should also be noted that with Orrin, only very low densities of data storage can be achieved. As data is stored by bit conversion of least significant bits of each byte in the media file then the maximum density of stored information in a file would be 17% if the least significant bit of each byte is converted. However, if the least significant bit of each byte is converted this dramatically compromises the security of the system of Orrin as someone trying to decode the data would know where to start looking.

Thus, the skilled person could in no way whatsoever, without invention, arrive at the present invention by starting at Orrin. It is only by making use of hindsight that one could even begin to put together the series of steps mentioned above.

Thus, it is submitted that the present invention as claimed in each of the independent claims 64, 65, 104, 115, 124 is both novel and inventive.

The newly added claims each recite in combination that the file index includes an indication of which parts of the data storage area are in use for storing the data set. This is in effect a "bit map" or "block allocation table" which indicates which physical parts of the data storage area are in use and cannot be used for storing further data sets. This facilitates proper management of the storage of multiple data sets either associated with a single file index or with multiple file indexes provided that these are all visible to the operating computer as the data sets are stored. This can help prevent collisions that can corrupt data.

As this "bit map" / "block allocation table" is encrypted and hidden as part of the file index, there is no tell tale sign left of the presence of data or any indication of the volume of data stored. There is no suggestion in the prior art to take this step or provide this advantage.

Note that claim dependent claim 128 has been drafted in recognition of the fact that besides varying the location of the file index by reference to a user passphrase similar advantages can be achieved by allowing the location to vary in other ways.

All outstanding issues have been addressed and this application is in condition for allowance. Should any minor issues remain outstanding, the Examiner should

contact the undersigned at the telephone number listed below so they can be resolved expeditiously without need of a further written action.

The Commissioner is hereby authorized to charge any deficiency, or credit any overpayment, in the fee(s) filed, or asserted to be filed, or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to our Account No. 14-1140.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: /Robert W. Faris/
Robert W. Faris
Reg. No. 31,352

RWF:ejs
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100